IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

123RF LLC, Plaintiff, v. HSBC BANK USA, N.A. Defendant.	**Case No. 21-cv-8519** **JURY TRIAL DEMANDED**

AMENDED COMPLAINT

Plaintiff, 123RF LLC ("Plaintiff"), for its amended complaint against Defendant, HSBC Bank USA, N.A. ("HSBC USA" or "Defendant"), alleges and states as follows:

NATURE OF THE ACTION

1. This case involves Defendant's grossly deficient security protocols and procedures, breach of fiduciary duties, breach of contract, and acts of fraud that permitted almost $1.5 million (and counting) in unauthorized Automated Clearing House ("ACH") debits from Plaintiff's commercial bank account to occur without Plaintiff's knowledge or consent, in direct violation of, among other things, the parties' contract and the respective duties Defendant, a commercial bank, owed to Plaintiff as its customer.

2. Plaintiff repeatedly contacted Defendant over a prolonged period of time to alert Defendant of the unauthorized ACH debits and attempt to put a stop to them. Defendant took months to even respond to Plaintiff, but ultimately failed to take any measures whatsoever to protect Plaintiff's funds.

3. Despite Plaintiff's repeated notice to Defendant of Defendant's security lapses, Defendant's security remains faulty and dangerous to Plaintiff and to the public—unbelievably,

months after Defendant was alerted to the unauthorized ACH debits, Defendant *continues* to process them, with the most recent unauthorized debits (as of the date of this amended complaint) occurring on September 16, November 12, December 16, and December 21, 2021. The November and December unauthorized debits occurred even after the original Complaint in this action was filed on October 15, 2021. This demonstrates Defendant's wanton and reckless disregard for Plaintiff's legitimate complaints concerning the security of its account and its funds, and reflects a continuing danger to Plaintiff and the public.

4. Importantly, Defendant has already admitted fault as it has returned $431,821.56 of the total $1,430,340.10 in unauthorized ACH debits to Plaintiff. Defendant continues to admit fault as it has also already refunded the amounts associated with the recent improper ACH debits from September to December 2021 referenced in the previous paragraph. Nonetheless, in violation of the parties' agreement, New York's Uniform Commercial Code, and common law, Defendant has refused to return the balance of $998,518.54.

5. Plaintiff brings this action to recover the damages it has suffered as a result of Defendant's malfeasance in an amount of no less than $998,518.54, plus punitive damages, statutory interest, and pre- and post-judgment interest.

THE PARTIES

6. Plaintiff, 123RF LLC, is a California limited liability company headquartered at 220 N. Green St., Chicago, Illinois 60607.

7. Defendant, HSBC Bank USA, N.A. is a full-service commercial bank headquartered at 452 Fifth Avenue, New York, New York 10018.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action based on 28 U.S. Code

§ 1332(a) because the amount of controversy exceeds the sum of $75,000, exclusive of interest and costs, and because the parties are diverse as defined by 28 U.S.C. § 1332(a)(1).

9. This Court has personal jurisdiction over the parties to this action pursuant to Sections 301 and 302 of the New York Civil Practice Law and Rules.

10. Defendant's principal place of business is located in New York, the events giving rise to this action took place in New York, and Defendant engages in a continuous and systematic course of doing business in New York because it maintains its headquarters in New York and regularly transacts business in New York.

11. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims in this action occurred in this district, and under 28 U.S.C. § 1391(d) because Defendant resides in this district.

FACTUAL BACKGROUND

12. Plaintiff 123RF LLC is a subsidiary of Inmagine Lab Pte. Ltd, which together with its affiliates forms the 123RF Group. The 123RF Group operates an online digital stock agency that sells royalty-free images, vectors, footage, and stock photography. 123RF Group has offices in 40 countries throughout the world.

13. 123RF Group's international headquarters is presently located in Singapore and its principal officers are based in Malaysia.

14. In 2012, 123RF Group formed Plaintiff to conduct business in the United States. Presently, Plaintiff is a wholly owned subsidiary of 123RF Limited, which is a wholly owned subsidiary of Inmagine Lab Pte. Ltd. As with other regional affiliates of 123RF Group, Plaintiff's management, accounting, and finance functions are managed by 123RF Group's Malaysian office, with just a handful of sales employees based in Plaintiff's Illinois office.

15. On or around August 7, 2012, Plaintiff opened a commercial banking account with HSBC USA ("Account") at HSBC Bank N.A. Fifth Avenue Office, 452 Fifth Avenue, New York, NY 10018. Plaintiff's understanding is that the relationship between Plaintiff and HSBC USA is governed by the US Commercial Deposit Account Agreement ("USCDAA"), attached hereto as Exhibit A.

16. The USCDAA required HSBC USA to "comply with the Security Procedures" and to "follow the Security Procedures upon receipt" of any payment instruction relating to the Account. "Security Procedures" were defined in the USCDAA as:

> [S]ecurity measures or protocols governing the Customer's access to the communication channels made available to the Customer by the Bank from time to time and used to verify the origination of Instructions or Communications between them transmitted by such channels. A Security Procedure may include, but is not limited to, one or more of the following measures: encryption algorithms or other codes, user entitlements, identifying words and numbers, and similar security devices.

17. The Security Procedures that applied to the Account are described more fully below.

18. Other companies within the 123RF Group also banked with HSBC's global subsidiaries, including in particular the Hong Kong Shanghai Banking Corporation Limited ("HSBC Hong Kong") and HSBC Bank Malaysia Berhad (collectively, "HSBC"). Until 2021, HSBC was 123RF Group's sole banking partner worldwide.

19. Defendant represented that it "works hard year round to protect [customer] information. We stay vigilant, identifying threats and investigating suspicious activity across all your accounts."[1] Defendant further represented that "[i]f we identify that your information has

[1] "Report Fraud - Security - HSBC Bank USA," accessed at https://www.us.hsbc.com/security/report-fraud/.

been compromised, we act promptly. We'll contact you directly and take the necessary steps to help safeguard your banking information."[2] Defendant represented that "we take responsibility – Holding ourselves accountable and taking the long view," and "we get it done – moving at pace and making things happen."[3] Plaintiff relied on Defendant's representations, which were determining factors in Plaintiff choosing Defendant as its primary banking provider. These representations were separate and distinct from Defendant's contractual obligations.

20. As discussed herein, these representations were false, as not only did Defendant not stay vigilant or identify Plaintiff's compromised assets, but Defendant also failed to act promptly once Plaintiff alerted Defendant of the serious security issues and, ultimately, took no steps whatsoever to protect Plaintiff's funds from continuing to be siphoned through unauthorized and unknown ACH debits. Defendant has not taken responsibility for its failures nor has Defendant held itself accountable for its improper siphoning of substantial funds from Plaintiff's Account (though it has already admitted fault by refunding a portion of the unauthorized debits). Defendant has also failed to "get it done" as it failed to respond to Plaintiff's complaints, nor did Defendant ever provide Plaintiff with a report of Defendant's purported internal investigation as Defendant claimed it would do. To this day, Defendant still has not responded to Plaintiff to explain why or how these improper debits occurred *and continue to occur despite Plaintiff's repeated complaints and this lawsuit*.

21. Plaintiff did not use the Account as a general commercial operating account. Instead, the Account was used to collect proceeds and settlements for online credit card sales in the United States, which were then transferred to accounts held by other 123RF Group entities as appropriate. These transfers were accomplished using direct wire transfers between 123RF

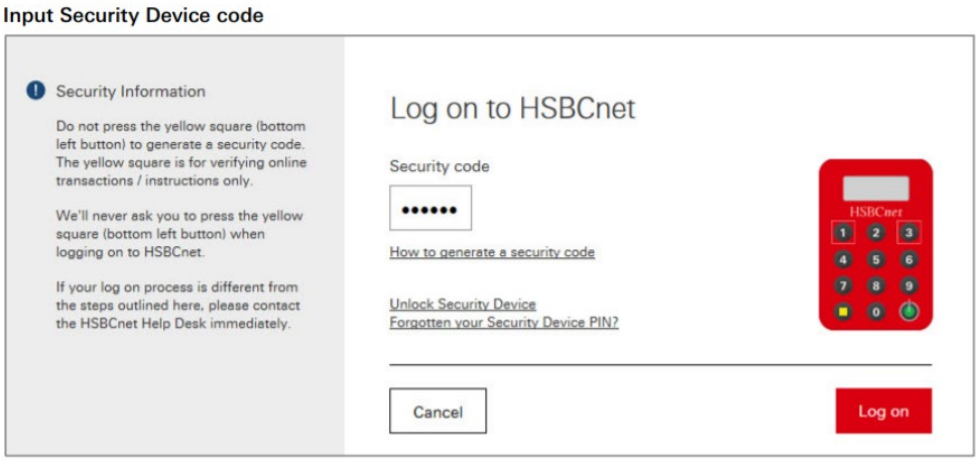
[2] *Id.*
[3] https://www.hsbc.com/who-we-are/purpose-values-and-strategy.

Group's HSBC accounts, initiated through the HSBCnet portal (a process described below), which Plaintiff understood was the only way to send funds from the Account. The Account was also used for a very limited set of administrative payments, such as to the Internal Revenue Service.

22. As mentioned above, Plaintiff's financial functions were performed by 123RF Group employees located in Malaysia. 123RF Group, HSBC USA, and Plaintiff had established the following Security Procedures for transfers involving the Account.

23. To initiate direct wire transfers, 123RF Group personnel had to follow a specific set of security procedures established for HSBC's online banking portal, HSBCnet. First, an employee authorized by 123RF Group to initiate direct wire transfers would log onto HSBCnet and enter payment details. Then, a designated authorizer – here, 123RF Group's chief executive officer – would log in to HSBCnet separately to approve the payment.

24. For security purposes, logging in to the portal required entering a one-time security token displayed on a small device issued by HSBC, which the bank refers to as a "Security Device." To receive a Security Device, an employee was required to apply for approval by both HSBC USA and Plaintiff. The image below, taken from materials published online by HSBC, shows a representation of the Security Device used to access the Account via HSBCnet and is pasted here for illustrative purposes.



25. When the Account was initially set up, an HSBC employee visited 123RF Group's offices in Malaysia to instruct employees on the use of the Security Device and the procedure to access the Account through the HSBCnet portal, and how to initiate and approve account transfers.

26. 123RF Group and Plaintiff understood these procedures to be the sole means to initiate transfers from the Account, and at no time did any HSBC employee suggest that any other procedures existed that were capable of initiating debits from the Account, including for ACH debits.

27. The ACH network is a centralized system used by participating financial institutions to process low-value batch transactions with the United States clearinghouse managed by the National Automated Clearing House Association ("NACHA").[4] ACH payment requests are collected by financial institutions throughout the business day, then transmitted to the ACH clearinghouse for net settlement.

28. The Account was only ever used to receive payments from credit card sales and

[4] NACHA, the National Automated Clearing House Association, is a trade group governing the ACH Network. Its Operating Rules are not posted publicly and must be purchased from NACHA.

issue payments through the HSBCnet portal, which the parties had established as the sole channel through which funds could be debited from the Account, not through ACH debits.

29. On information and belief, there is no mechanism through which Plaintiff can initiate nor authorize an ACH transfer through the HSBCnet portal.

30. Importantly, at no point did anyone at 123RF Group ever initiate an ACH debit using the Account.

31. Yet, as described herein, HSBC USA improperly, and without Plaintiff's authorization or knowledge, processed hundreds of ACH debits from the Account that were not initiated through the HSBCnet portal. It is as if Plaintiff contracted with HSBC USA for the use of a secured bank vault, with HSBC USA establishing with Plaintiff a rigorous multi-step process to open the vault's foot-thick steel door, but all the while anyone could access the vault through an unlocked screen door at the back.

32. In early April 2020, as 123RF Group's finance department completed its reconciliation of Plaintiff's January and February 2020's management accounts, the finance department began to notice odd ACH debits initiating from the Account. These transactions appeared multiple times a week, virtually all as online payments to credit card companies. (Attached hereto as Exhibit B is a schedule showing the total amounts debited to each recipient as of October 15, 2021). The amounts transferred generally ranged from around the low hundreds to the low thousands of dollars, though the largest transactions reached $25,000. Plaintiff identified, among other payments, over $360,000 in debits to Discover E-Payments; $259,000 to Macy's Online CC; and nearly $150,000 to Wells Fargo CC.

33. The ACH network has long been a target of third-party scammers and fraudsters, According to FICO, a data analytics firm that pioneered the use of individual credit scores, the

prevalence of fraudulent ACH activity increased substantially from 2019 to 2021.

34. Indeed, NACHA recently implemented the WEB Debit Account Validation Rule, set to be implemented March 2021 but delayed a year due to the Covid pandemic, to target a recent increase in ACH fraud. The rule, which applies to consumer accounts, requires banks to conduct validation steps before initiating ACH debits for consumer accounts. For commercial accounts, NACHA already requires banks to use commercially reasonable fraud detection systems to identify and prevent fraudulent ACH transfers.

35. On information and belief, the unauthorized transactions bore many hallmarks that HSBC USA should have recognized as signaling the ACH transfers were fraudulent, including among other things that the transfers began abruptly in high volume out of pattern with prior activity on the Account; that the recipients of the transfers were distinct from the intracompany recipients of Plaintiff's legitimate direct wires; and the character of the payment amounts and payment recipients. On information and belief, had Defendant employed commercially reasonable fraud detection methods, Defendant would have identified these transfers as fraudulent and promptly blocked them and alerted Plaintiff. It is also a certainty that the transfers could not have occurred if Defendant had not allowed transfers to occur outside the security procedures associated with accessing the HSBCnet portal.

36. Upon discovery of the unauthorized debits, 123RF Group conducted an internal investigation to determine what occurred. At approximately the same time, Plaintiff also alerted Defendant to the issues and requested that Defendant conduct its own internal investigation and report on its findings. 123RF Group interviewed employees and executives across the organization to determine if any of the transactions were legitimate, or if there were any dishonest employees within the organization who had initiated or facilitated these transactions.

(The time necessary to conduct these investigations was impacted by the early stages of the ongoing Covid-19 pandemic, which had just begun in Spring 2020).

37. The results of the investigation were consistent—123RF Group found no indication that any of the payments had been authorized or executed by anyone at 123RF Group or Plaintiff, and found no indication that there were any dishonest employees within the organization involved with these unauthorized transactions.

38. In fact, 123RF Group's investigation confirmed 123RF Group's understanding that these improper ACH debits could only have been caused by Defendant. First, 123RF Group was not aware that the Account could generate ACH debits. Second, 123RF Group's investigation confirmed their understanding that the only way for payments to be made out of the Account was through a multi-step security procedure through the HSBCnet portal.

39. This process included four levels of control and segregation of duties in executing a payment transaction. First: Finance Department Staff were only allowed to set up payment details, such as amount and beneficiary bank account and approved supporting documents. Second: Wong Eng Eng ("Ms. Wong"), Senior Finance Manager would verify the transaction. Third: Leong Choong Wah ("Mr. Leong"), the CFO, would conduct a final check and approval of the transaction. Fourth: The founders, directors, or ultimate beneficial owners of Plaintiff would, as Executors and Authorizers ("Authorized Signatories"), execute the payment.

40. These payments could not be executed by finance department staff. These payments could only be executed by the Authorized Signatories who held the HSBCnet portal tokens and had access to the Account through password controls. The investigation revealed and confirmed that approval and transfer of funds would have to have been conducted by multiple parties and it would be impossible for any "dishonest employee," for example, to steal any such

funds independently.

41. During 123RF's investigation, the Authorized Signatories confirmed that they maintained control of their issued Security Devices at all times, and that nobody else had access to the devices. The Authorized Signatories also all confirmed that they were unaware of any process to initiate an ACH transaction or initiate payments from the account except through the process described above.

42. Moreover, while Plaintiff requested that Defendant conduct its own investigation and report on their findings, Defendant never did so. Defendant never provided Plaintiff with the process flow of how Plaintiff's funds left its account—indeed, Defendant did not even begin providing Plaintiff with notifications of ACH debits until *after* Plaintiff alerted Defendant to the unauthorized transfers.

43. To this day, and even at a conference before the Court on January 10, 2022, Defendant claims it does not know what happened, yet it continues to permit such unauthorized ACH debits through a means other than through the HSBCnet portal.

44. Defendant also continues to admit liability for these improper transactions.

45. Since the filing of the original complaint in this action in October 2021, Defendant has refunded the unauthorized ACH payments that continue to occur.

46. This is pure and unequivocal evidence of Defendant's guilt, as well as Defendant's reckless disregard of, and failure to take any steps to correct, the issue Plaintiff timely presented to Defendant.

47. These unauthorized ACH debits had not been initiated through the HSBCnet portal. In fact, Plaintiff had not even been aware that debits *could* be initiated from the Account without going through HSBCnet—that security feature was a main reason why Plaintiff chose

this account type. Nor could Plaintiff find any indication that anyone at HSBC had ever sent any transaction authorization requests or notices of any kind to Plaintiff prior to executing the transactions.

48. By August 2020, over $322,000 had been taken from Plaintiff through unauthorized ACH debits..

49. In August 2020, having not heard from HSBC USA, Ms. Wong attempted to get Defendant's attention by contacting the general HelpDesk line for HSBC USA about the situation and sought to obtain the contact information for the account relationship manager overseeing Plaintiff's Account. The customer service agent who answered was unable to help, but promised to identify the proper account relationship manager and call back. Nobody ever called back.

50. In November 2020, Plaintiff turned to the account relationship manager for 123RF Group's HSBC Hong Kong accounts, Ms. Sallynne W.K. Yuen ("Ms. Yuen"). Ms. Yuen—who was transitioning out of her role as 123RF Group's HSBC Hong Kong account relationship manager—initially offered to help locate the account relationship manager for the Account. However, despite repeated follow-up emails and calls she did not provide a contact either.

51. Meanwhile, the unauthorized ACH payments continued. Indeed, by March 2021 the unauthorized ACH transactions totaled over $1.4 million. The rate of the transfers had accelerated over time.

52. On January 21, 2021, three 123RF Group employees received an email from Mr. Kwok Cheung ("Mr. Cheung"), introducing himself as the company's new HSBC USA account relationship manager. Plaintiff immediately responded. However, as the email made no

reference to Plaintiff's efforts to get in contact, Plaintiff was initially concerned with a phishing attempt. Plaintiff reached out to Ms. Yuen to confirm Mr. Cheung's identity. A week passed without confirmation, and on January 27, 2021, Ms. Yuen told 123RF "there are still documents to finalize internally before I could share information to him. Suggest you to hold off until I confirm."

53. In February 2021, Ms. Bonnie Ho ("Ms. Ho") took over from Ms. Yuen as 123RF's Group HSBC Hong Kong account relationship manager, and for the first time confirmed that Mr. Cheung was in fact an HSBC USA's employee. She thereafter attempted to liaise between Plaintiff and HSBC USA, but HSBC USA remained slow to communicate. Finally, Plaintiff and 123RF Group had connected with an individual at HSBC USA to whom they could request that the bank stop the unauthorized ACH transfers debiting the Account.

54. On March 17, 2021, 123RF Group's chief financial officer Mr. Leong forwarded to Mr. Cheung an Excel spreadsheet identifying each unauthorized transaction, by then over $1.4 million in unauthorized ACH debits. Mr. Leong requested Mr Cheung's help in stopping the payments and recovering their lost funds.

55. Ms. Ho stepped in as well to reiterate the urgency of the request. By email dated March 25, 2021, Ms. Ho confirmed to Mr. Cheung that Plaintiff had requested HSBC USA stop all transactions for the Account until an investigation could be completed, and requested HSBC USA identify any steps Plaintiff needed to complete to stop the unauthorized transactions.

56. At Mr. Cheung's request, Plaintiff resubmitted the disputed transactions using HSBC USA's transaction dispute form (the PDFs totaled 86 pages) and Ms. Wong filed a report with the Chicago Police Department, dated March 26, 2021. Plaintiff understood from HSBC USA's comments that these were necessary steps to be reimbursed for the unauthorized ACH

payments.

57. Despite Plaintiff's clear communication to Defendant, and Defendant's undisputed knowledge of the severity of the issue, unauthorized ACH transactions continued to be debited from the Account. Normal practice would be for HSBC USA to transfer Plaintiff's Account to a new account number, cutting off whomever was initiating the unauthorized transactions. HSBC USA did not do this, nor did it suspend ACH functionality on the Account. Instead, on March 30, 2021, Plaintiff began receiving auto-generated email alerts as each unauthorized ACH transaction was initiated, asking that the recipient approve or deny the transaction. In all cases Plaintiff denied the transactions.

58. Plaintiff was puzzled and frustrated when they learned these emails were being sent. First, Plaintiff could not understand why similar emails had not been sent to 123RF Group before HSBC USA executed over $1.4 million in unauthorized ACH debits. Second, Plaintiff had been clear that no ACH transactions from the Account would be legitimate, so did not understand why they were being asked to approve or deny additional ACH transfers one-by-one. Third, the approval emails were directed at a junior administrative employee (who never approved any of the debits), not one of the limited individuals that Plaintiff and 123RF Group had identified to HSBC USA as having the authority to approve transactions involving the Account.

59. The USCDAA had obligated HSBC USA to "use its reasonable efforts to comply with any request made by the Customer to vary or cancel an Instruction," with "Instruction" defined as a communication with sufficient information to initiate a transaction. Despite Plaintiff's instruction to HSBC USA to void all ACH transfers, HSBC failed to comply with this request and continued to process unauthorized transactions.

60. On April 16, 2021, Mr. Leong and Ms. Wong had a Zoom online meeting with Mr. Cheung. At the meeting, Mr. Leong requested Mr. Cheung's prompt attention to recovering the funds lost through the unauthorized transfers. During the meeting, Mr. Cheung did not rebut 123RF Group's chief financial officer's claims on the unauthorized ACH transactions. According to Mr. Cheung, HSBC USA was aware of similar unauthorized ACH transactions affecting other HSBC USA customer accounts. Mr. Cheung also advised on the procedure to recover the entire unauthorized transactions of $1.4 million.

61. Around this same time, in April 2021, HSBC USA provided its response to Plaintiff's dispute applications and request for reimbursement. While the bank reimbursed $431,821.56 of the total $1,430,340.10 lost to the transactions, they refused to return the balance of $998,518.54. The reimbursed transactions had all occurred in March and April 2021, though some transactions within that range were not reimbursed. HSBC USA had not previously informed Plaintiff that any portion of the debited funds would not be returned.

62. Plaintiff disputed HSBC USA's refusal to reimburse the total amount lost. On April 20, 2021, Client Service Manager Adam Anthon ("Mr. Anthon") told Plaintiff that "[m]any of the fraudulent transactions have already been returned" and the bank would not return the lost funds because most of the unauthorized transactions "are outside of the NACHA guidelines and we would not be able to recover them."[5] Asked to elaborate, he added, "[w]e would not be able to recover the funds per the NACHA guidelines all banks have to follow for attempting to recall/reverse an ACH payment. It is very difficult to recover a payment if more than one business day has passed."

63. On April 22, 2021, in response to a follow-up email from Ms. Ho, Mr. Anthon

[5] The NACHA Operating Rules are not posted publicly and must be purchased from NACHA.

stated that while Plaintiff had "never initiated any ACH credit payments via HSBCnet," he claimed that "[Plaintiff] has authorized 3rd party debits via ACH over the history of the account." This was untrue—Plaintiff had *never* authorized an ACH transaction via HSBCnet, the sole portal through which 123RF Group interacted with the Account. In fact, after receiving Mr. Adam's email 123RF Group personnel attended another Zoom meeting with Mr. Cheung, where they requested documentary evidence that Plaintiff had ever authorized an ACH transaction and a copy of the investigation report. No evidence or investigation report was ever provided.

64. On information and belief, Defendant intentionally did not respond to Plaintiff's requests to immediately service the Account and rectify the unauthorized ACH debits to permit this so-called one-business-day rule, which Plaintiff was never aware of and dispute, to lapse.

65. Assuming *arguendo* Defendant's fabricated one-day-rule did exist, it then had an even greater duty to respond immediately to Plaintiff's timely requests for servicing, which Defendant failed to do.

66. Instead, on April 27, 2021, Mr. Cheung reiterated Mr. Anthon's April 22, 2021's statement that because Plaintiff had not paid for a "Debit block service," HSBC USA's policy was to allow ACH debits to be taken from the account—apparently regardless of authorization from the customer—and would not notify the customer. As mentioned above, there is no apparent mechanism to initiate ACH transfers through the HSBCnet portal, the only procedure authorized by the parties to initiate debits from the Account. This meant that *any* ACH transfers from the Account were *a priori* unauthorized, a fact that HSBC USA was at all times aware of. Thus, what Mr. Anthon and Mr. Cheung were admitting was that it was HSBC USA policy to *knowingly allow* unauthorized transfers to deplete a customer's account unless the customer paid

an additional fee.

67. In further discussions, HSBC USA also continued to claim that "NACHA guidelines" prevented reimbursement of the unauthorized transactions, and that the bank "typically" cannot recover payment after one business day.

68. To be clear, the only procedure Plaintiff authorized for debiting the Account was through the secure HSBCnet portal and its multi-step security process. Plaintiff did not know that there were other non-secure ways for debits to be transferred from the Account. In all events, Plaintiff never authorized any ACH debit nor did Plaintiff know of any unauthorized ACH debits until after the unauthorized transaction had been completed.

69. The HSBCnet portal does not support ACH debits. As such, there should not been any ACH debits on the Account at all because Plaintiff never authorized any debits outside of the HSBCnet portal. Thus, all ACH debits initiated outside of the HSBCnet portal should have automatically been rejected by Defendant because all ACH debits on the Account were unauthorized, *quod erat demonstrandum*.

70. HSBC USA was at all times aware of these facts. Thus, what Mr. Anthon and Mr. Cheung were admitting was that it was HSBC USA's policy to *knowingly allow* unauthorized transfers to deplete a customer's purportedly secure account unless the customer paid an additional fee for the "Debit block service" to protect against HSBC USA's self-manufactured and undisclosed security breach.

71. In further discussions, HSBC USA also continued to claim that "NACHA guidelines" prevented reimbursement of the unauthorized transactions, and that the bank "typically" cannot recover payment after one business day. At no point did HSBC USA identify the "NACHA guidelines" that supposedly authorized it to refuse reimbursement, or specify when

and how Plaintiff had agreed to be bound by these so-called "NACHA guidelines."

72. For instance, by letter dated July 12, 2021, HSBC USA Senior Manager Ms. Lynne Mitchell Mische ("Ms. Mische") called the remaining $998,463.56 in unauthorized payments "unrecoverable," because Plaintiff "did not inform HSBC Bank USA, National Association (HSBC USA) of the unauthorized transactions within the afforded time frames established under NACHA Operating Rules." Ms. Mische did not specify what the "afforded time frames" established under "NACHA Operating Rules" despite Plaintiff's notification to HSBC USA.

73. On information and belief, there is no "NACHA Guideline" or other law or regulation that would prevent HSBC USA from reimbursing to Plaintiff the unauthorized transfers it improperly allowed to be debited from the Account.

74. By letter dated July 28, 2021, counsel for Plaintiff demanded, among other things, that HSBC USA provide a copy of the agreements that the bank asserts as governing the relationship between the parties. As is typical in modern transactions with large consumer-facing institutions, the HSBC USA documents executed by Plaintiff referred to terms of service provided in other documents, which are no longer publicly available.

75. On August 24, 2021, HSBC USA responded through Mr. Michael Mendola ("Mr. Mendola"), Associate General Counsel at HSBC Bank USA, N.A. Mr. Mendola refused to reimburse the outstanding amounts owed. Mr. Mendola also asserted that HSBC USA would not make any efforts to preserve documents relating to the dispute as requested by counsel for Plaintiff, suggesting that the bank intended to spoliate whatever relevant documents might exist.

76. Mr. Mendola declined to identify to Plaintiff the agreement terms that HSBC USA believes to govern the contractual relationship between the parties. Instead, Mr. Mendola

asserted that the parties contract terms "are governed by and interpreted according to, inter alia, the . . . [NACHA] Operating Rules," which he asserted required Plaintiff to alert HSBC USA of unauthorized transactions within "one business day of the settlement date." Mr. Mendola did not attempt to identify where, when, or how Plaintiff agreed to be governed by NACHA "Operating Rules" (which are not publicly available), either in general or specifically with regard to unauthorized transfers; what specific NACHA rules imposed this purported requirement to notify HSBC USA of unauthorized ACH debits within one business day; or how these purported rules were capable of superseding New York State Law.

77. The HSBC USA Rules for Commercial Deposits, which Plaintiff understands to apply to the Account, references NACHA guidelines once, in a section titled "Notice of Receipt of ACH Payments." This section, which refers to cases where the customer *receives* payments, states that "Under the operating rules of the National Automated Clearing House Association . . . the Bank is not required to give next day notice to you of receipt of an ACH item."

78. Mr. Mendola's letter also added that "this response is submitted with prejudice," which Plaintiff understood to mean that HSBC USA refuses to engage in any further discussion regarding the matter.

79. This is not the first time Defendant has had security protocol failures and put its bottom line ahead of the needs of its customer. Indeed, according to a 2010 Forrester Research study, Defendant was rated the worst bank in customer advocacy. In response to the question: "My financial provider does what's best for me, not just its own bottom line," Defendant received the lowest rating by far of 16%, which was 10% lower the previous year.

80. Incredibly, *several additional* illicit and unauthorized ACH debit occurred on September 16, November 12, December 16, and December 21, 2021, debiting the Account

another $900, $261.03, $900, and $900, respectively. The November and December unauthorized transfers occurred after Plaintiff filed its original Complaint in this action in October 2021.

81. These additional improper ACH debits occurred despite HSBC USA's knowledge of the serious security issues concerning the illicit and unauthorized ACH debits from Plaintiff's Account (and as a result all accounts similar to Plaintiff's account) for more than a year; the parties' Agreement concerning the Account protocols including what should have been an automatic denial of any ACH debits; Plaintiff 's demand to freeze its account; and Plaintiff's explicit order confirming with HSBC USA that no ACH debits were permitted on the Account.

82. Incredibly, HSBC USA processed more than one of these ACH transactions *without* sending an automated approval email of the type that had begun arriving in March 2021, and despite the transaction leading the Account to be overdrawn. (123RF Group had been keeping only a minimal balance in the Account in the hope that HSBC USA might stop processing ACH debits if the balance was too low to cover them.)

83. HSBC USA failed to send Plaintiff any contractually required Letter of Authorization to lift the security freeze over the Account, nor did HSBC USA provide any request or alert to Plaintiff prior to this most recent unauthorized ACH debit.

84. Despite Defendant's knowledge and admission of fault, Defendant shockingly continues to approve unauthorized ACH debits to Plaintiff's detriment, and refuses to pay Plaintiff the damages Defendant knows it has caused to Plaintiff.

85. On October 15, 2021, Plaintiff filed a Complaint against Defendant in this Court.

86. On December 13, 2021, Defendant filed and served a letter requesting a pre-motion conference with the Court regarding a planned motion to dismiss.

87. On January 10, 2022, the parties attended a pre-motion conference before the Court.

88. On January 24, 2022, the parties entered into a stipulation setting filing and briefing dates, including setting February 14, 2022 as the last day for Plaintiff to file its amended complaint.

FIRST CLAIM FOR RELIEF

BREACH OF N.Y. U.C.C. § 4-A-204(1)

89. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

90. From November 2019 until April 2021, HSBC USA accepted payment orders issued in the name of Plaintiff, which were neither authorized by Plaintiff nor otherwise effective or enforceable.

91. Plaintiff exercised ordinary care to determine that the ACH debits were not authorized by Plaintiff and notified HSBC USA of each of the unauthorized transactions within a reasonable time, never exceeding thirty days after the dates Plaintiff finally began receiving email notifications from HSBC USA that Plaintiff's Account was being debited through unauthorized ACH debits.

92. The unauthorized ACH debits totaled $1,430,340.10. While Defendant reimbursed $431,821.56 of unauthorized transactions, Defendant refused to return the balance of $998,518.54.

93. In all events, Plaintiff notified HSBC USA of each of the unauthorized transactions within one year of their occurrence.

94. HSBC USA knowingly accepted these orders and debited Plaintiff's account

because it did not implement the agreed security procedures for the Account and/or failed to apply commercially reasonable security procedures, including in particular, Defendant's (a) failure to require that the transactions be initiated through the HSBCnet web portal, (b) failure to receive authorization from the 123RF employees designated to give authorization, (c) failure to provide notice that the transactions had occurred, (d) failure to identify suspicious patterns in Account activity, and (e) failure to make representatives available to receive alerts of unauthorized debits.

95. Further, pursuant to Section 4A–203(a)(1), HSBC USA, through the USCDAA, agreed to bear responsibility for unauthorized transfers where, as here, HSBC USA failed to follow agreed security procedures and where the unauthorized transfers did not result from any security lapse by Plaintiff.

96. Plaintiff is entitled to damages in the amount of all unauthorized ACH transactions improperly processed by HSBC USA, equaling $998,518.54.

97. Plaintiff is also entitled to interest on the refundable amount calculated from the date Defendant improperly authorized the transactions to the date of the refund at the rate set forth in N.Y. U.C.C. § 4-A-506. As such, Defendant is obligated to pay Plaintiff interest on the already refunded amount of $431,821.56 from the dates of the unauthorized ACH debits to the date of the refund. Additionally, Defendant is obligated to pay Plaintiff interest on the yet to be refunded amount of $998,518.54 from the dates of the unauthorized ACH debits to a date in the future when Defendant refunds the money to Plaintiff.

98. Plaintiff is also entitled to receive pre- and post-judgment interest on the total amount awarded.

99. As a result of Defendant's actions, Plaintiff has suffered, and continues to suffer,

damages.

SECOND CLAIM FOR RELIEF

GROSS NELIGENCE

100. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

101. Defendant owed a duty to Plaintiff to act as a reasonably prudent commercial banking company would act.

102. The unauthorized ACH payments totaled $1,430,340.10. While Defendant reimbursed $431,821.56 of unauthorized transactions, Defendant refused to return the balance of $998,518.54.

103. Through the actions described above, Defendant grossly breached its duties by, among other things, recklessly, willfully, and wantonly: failing to follow internal procedures on the Account; failing to require all debits to follow the multi-step security procedures required by the HSBCnet web portal; failing to require that the transactions be initiated through the HSBCnet web portal; failing to receive authorization from the Plaintiff employees designated to give authorization; failing to provide Plaintiff with notice that the transactions had occurred; accepting the fraudulent orders and debiting Plaintiff's account even after Plaintiff provided notice to Defendant that all ACH debits were unauthorized; failing to identify suspicious patterns in Account activity; failing to make representatives available to receive alerts of unauthorized payments; failing to have and implement proper controls needed to prevent the actions described above from taking place; failing to properly monitor Plaintiff's Account; failure to put the Account on hold once notified of fraudulent transactions; failure to cancel the Account and create a new account once notified of fraud; and continuously and knowingly allowing funds to

be fraudulently debited from the Account.

104. As a result, Plaintiff was damaged by an amount of no less than the sum of the unreimbursed ACH debits processed by Defendant.

105. The actions complained of herein were taken recklessly, willfully, and wantonly such that the imposition of punitive damages is warranted as a result of Defendant's gross negligence.

THIRD CLAIM FOR RELIEF

NELIGENCE

106. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth therein.

107. Defendant owed a duty to Plaintiff to act as a reasonably prudent commercial banking company would act.

108. The parties agreed that HSBC USA would implement higher level security procedures before payments orders issued in the name of Plaintiff would be executed. These procedures included in particular the requirement that payment orders for Account debits be issued through the HSBCnet portal, requiring the use of a one-time security token.

109. Through the actions described above, Defendant breached its duties by, among other things, failing to follow internal procedures on the Account, failing to follow the multi-step security procedures required by the HSBCnet web portal, failing to require that the transactions be initiated through the HSBCnet web portal, failing to receive authorization from the Plaintiff employees designated to give authorization, failing to provide Plaintiff with notice that the transactions had occurred, accepting the fraudulent orders and debiting Plaintiff's account, failing to identify suspicious patterns in Account activity, failing to make representatives

available to receive alerts of unauthorized payments, failing to have and implement proper controls needed to prevent the actions described above from taking place, failing to properly monitor Plaintiff's Account, and allowing funds to be removed from the Account without authorization.

110. As a result of Defendant's actions, Plaintiff was damaged by an amount no less than the sum of the unreimbursed ACH debits processed by Defendant.

FOURTH CLAIM FOR RELIEF

BREACH OF CONTRACT

111. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

112. Plaintiff entered into a valid and enforceable contract with Defendant. In consideration of monetary compensation paid by Plaintiff, Defendant provided commercial banking services in the form of the Account. Plaintiff understands the terms of this agreement to be consistent with the HSBC US Commercial Deposit Account Agreement.

113. The USCDAA required HSBC USA to follow the Security Procedures in transactions involving the account. The agreement also required HSBC to "use its reasonable efforts to comply with any request made by the Customer to vary or cancel an Instruction."

114. Plaintiff fully performed all of its obligations under these agreements including abiding by proper security procedures for the Account, monitoring the account, attempting to promptly report the suspect ACH transactions after investigation, and following all instructions of Defendant once the Defendant responded to Plaintiff's complaints.

115. Defendant breached its contract with Plaintiff by, among other things, executing unauthorized ACH debits in contravention of agreed security procedures, failing to notify

Plaintiff prior to executing these debits, failing to provide a proper channel to report unauthorized ACH debits, failing to promptly move Plaintiff's Account to a new account number after being notified of the fraud, failing to block ACH transfers after being notified of the fraud, failing to provide Plaintiff with a secure Account, and failing to pay Plaintiff for the full amount of unauthorized debits.

116. As a result of Defendant's breach, Plaintiff has been damaged, and continues to be damaged, by an amount of no less than the sum of the unreimbursed ACH debits processed by Defendant.

FIFTH CLAIM FOR RELIEF

VIOLATION OF N.Y. G.B.L. § 349

117. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

118. As described herein, Defendant's consumer-oriented practices of, *inter alia*: (1) refusing to compensate customers for unauthorized ACH debits, based on alleged hidden terms that purportedly govern the parties' agreement; (2) intentionally permitting ACH debits without authorization because an additional fee was not paid (nor requested) for debit-blocking service that Plaintiff understood already existed in the Account based on the type of account; and (3) duping the consumer into believing their account was secure against unauthorized ACH debits in light of the multi-step debit process required via the HSBCnet portal, are deceptive acts or practices within the meaning of New York General Business Law § 349. Plaintiff understands that other members of the public continue to be subject to these deceptive acts and practices.

119. Defendant's deceptive practices were misleading in a material way. Plaintiff was induced to utilize Defendant's banking services and open the Account under the misleading

guise that their Account was secure against unauthorized ACH debits.

120. Defendant's violation of this statute is willful and knowing.

121. As a result of Defendant's violation, Plaintiff has been damaged in the amount of the balance of ACH debits improperly processed by Defendant and not yet reimbursed.

SIXTH CLAIM FOR RELIEF

BREACH OF FIDUCIARY DUTY

122. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

123. Defendant was a fiduciary of Plaintiff by nature of the relationship whereby Plaintiff trusted and relied on the expertise of Defendant to manage Plaintiff's funds.

124. Defendant breached its fiduciary obligations by, *inter alia*, failing to follow internal procedures on the Account, failing to contact Plaintiff about the unauthorized ACH debits taking place in its Account, and taking Plaintiff's monies and knowingly allowing funds to be removed from its Account without proper authorization.

125. As a result of Defendant's breach, Plaintiff was damaged by an amount no less than the sum of the unreimbursed ACH debits processed by Defendant.

126. The actions complained of herein were taken willfully and wantonly such that the imposition of punitive damages is warranted.

SEVENTH CLAIM FOR RELIEF

FRAUD

127. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

128. Defendant represented that the Account Plaintiff signed up for with Defendant

had security measures and controls in place to protect against unauthorized debits, such as the multi-step protocol set forth on the HSBCnet portal. Defendant further represented that it stays vigilant, identifies threats, and investigates suspicious activity across all accounts. Defendants further represented that if it knows of a threat, it will act promptly, contact Plaintiff directly, and take necessary steps to help safeguard Plaintiff's banking information.

129. These representations were material to Plaintiff and were key to Plaintiff permitting Defendant to continue to manage Plaintiff's assets.

130. These statements were false, and Defendant was aware of the falsity of the statements when they were made.

131. Defendant also made fraudulent omissions. Defendant was aware that the Account lacked security measures that would protect Plaintiff from all ACH debits, and intentionally failed to disclose this information to Plaintiff in order to induce Plaintiff into first acquiring the Account and then requiring Plaintiff, albeit unknown to Plaintiff, to pay for an additional ACH blocking service, in a bait and switch scheme that should not have been necessary under the original representation by Defendant concerning the strong security structure of the Account.

132. The statements and omissions were made with the intention that Plaintiff rely upon them, and Plaintiff did rely on such statements to their detriment.

133. Defendants knowingly authorized fraudulent ACH debits to Plaintiff's Account.

134. As a result of Defendant's actions, Plaintiff was damaged by an amount no less than the sum of the unreimbursed ACH debits processed by Defendant.

135. The actions complained of herein were taken willfully and wantonly such that the imposition of punitive damages is warranted.

EIGHTH CLAIM FOR RELIEF

BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

136. Plaintiff repeats and realleges the allegations in the preceding paragraphs as if fully set forth herein.

137. The contract between Plaintiff and Defendant contains an implicit covenant of good faith and fair dealing.

138. As described herein, Defendant breached that covenant and acted to deprive Plaintiff of benefits under the contract and wrongfully enrich Defendant.

139. As a result, Plaintiff was damaged by an amount no less than the sum of the unreimbursed ACH debits processed by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendant as follows:

1. All actual damages caused by Defendant's actions to be determined at trial, but in all events at least $998,518.54;
2. Restitution;
2. Punitive damages;
3. Its reasonable and necessary attorneys' fees for prosecuting this action;
4. Pre- and post-judgment interest at the highest lawful rate;
5. Costs of suit; and
6. Such other and further relief to which Plaintiffs may be justly entitled.

JURY DEMAND

Plaintiff hereby demands trial by jury on all issues.

Dated: New York, New York
February 14, 2022

Respectfully submitted,

FENSTERSTOCK, P.C.

By: /s/ Evan S. Fensterstock
Evan S. Fensterstock (EF2084)
efensterstock@fensterstockesq.com
200 Vesey Street, 24th Floor
New York, New York 10281
Telephone: (212) 859-5026

LEWIS & LLEWELLYN LLP

By: /s/ Tobias Snyder
Paul T. Llewellyn (CA Bar No. 216887) (*admitted pro hac vice*)
Tobias Snyder (TS3552)
Evangeline A.Z. Burbidge (CA Bar No. 266966) (*admitted pro hac vice*)
pllewellyn@lewisllewellyn.com
tsnyder@lewisllewellyn.com
eburbidge@lewisllewellyn.com
601 Montgomery Street, Suite 2000
San Francisco, California 94111
Telephone: (415) 800-0590

Attorneys for Plaintiff